REMARKS

Claims 1 – 126 are pending in the application. Claims 1, 69, 109, 110, 125 and 126 are currently amended. New claims 127 and 128 are added.

Claim Rejections – 35 USC 112

The Examiner rejected claim 125 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. More specifically, the Examiner is of the opinion that it is not clear where the term "prepossessed content" is found in the specification.

The term "prepossessed content" no longer appears in claim 125.

It is therefore believed that claim 125 complies with the written description requirement, and that claim 125 should be allowed.

Claim Rejections – 35 USC 102 & 103

The Examiner rejected Claims 1-4, 11, 51, 56-65, 69, 70, 109-112, 125 and 126 under 35 USC 102(e) as being anticipated by Kephart US Patent No. 6,732,149.

The Examiner further rejected claims 69, 70, 73, 86, 87, 91-99 under 35 USC 103(a) as being unpatentable over Kephart US Patent No. 6,732,149 in view of Olnowich US Patent No. 6,389,476.

Favorable reconsideration of this rejection in view of the above amendments and the following explanations is respectfully requested.

Claim 1, as currently amended, defines a system for network content monitoring of a *local or organizational* network, comprising:

a transport data monitor, connectable to a point in said network, for monitoring data being transported past said point,

a description extractor, associated with said transport data monitor, for extracting descriptions of said data being transported,

a database of at least one preobtained description of known content whose movements it is desired to monitor,

said content being internally generated in the network in advance of said extracting, said preobtained description being obtained in advance of said extracting descriptions, and

a comparator, configured to determine whether said extracted description corresponds to any of said at least one preobtained descriptions, *said corresponding being in accordance with a confidence level*, and to decide, *using said confidence level,* whether said data being transported comprises any of said content whose movements it is desired to monitor according to said determining.

As defined by claim 1, the present application describes a system for network content monitoring and control of a local or organizational network. This term in the preamble is imported into the claim limitations and therefore narrows the broadest reasonable interpretation to allow the Internet generated spam of Kephart to be excluded from the scope of the claims.

The system described by the present application relates to the monitoring of digital content, for enforcing copyright, secrecy, and confidentiality with respect to the transported digital content. The present application defines in the field of invention section: "The present invention relates to monitoring transport of digital content, particularly but not exclusively for the enforcement of digital copyright, secrecy, and confidentiality".

The present application introduces the novel and inventive idea of controlling the movement of content of known documents, internally generated in the organization's network, based on a comparison made by a comparator where the comparator is configured to determine whether said extracted description corresponds to any of said at least one preobtained descriptions, *said determining further comprising a confidence level,* and to decide, *using said determination with said confidence level,* whether said data being transported comprises any of said content whose movements it is desired to monitor according to said determining.

The amendment is based on the teachings in paragraphs 0175 – 0177, where it is taught *inter alia* that the signatures are compared with those of the database and for each match the confidence level is increased. It is further taught that the sequential and batch decision modules serve as inputs to a final decision module which estimates a final probability; this too would constitute a confidence level of the kind referred to in the claim.

The confidence level claimed is also based on the teaching in the disclosure of an entropy measure being used to provide a confidence level. As disclosed a high entropy indicates a high probability of encrypted data being present. Encrypted data may well be content it is desired to restrict and therefore needs to be stopped. Thus even if the signatures are not matched (because the signatures are based on unencrypted versions), if the confidence level indicates encryption then the content may be stopped or investigated further. The feature of encrypted data was already taught in claim 30 which was rejected over a combination of Kephart and Thomlinson. Thomlinson however does not teach detection of the presence of encryption based on entropy levels, nor the does he teach the generalization of the detection of the presence of encryption according to a confidence level. He therefore

does not teach determining whether content corresponds to content it is desired to protect according to a confidence level. The missing feature here is not taught in Kephart either, which does not teach confidence levels.

Kephart General Comments

Kephart US Patent No. 6,732,149 teaches a system and a method for protection against SPAM, as described in the field of invention section: "the present invention relates to a system and method for automatically detecting and handling unsolicited and undesired electronic mail such as Unsolicited Commercial E-mail (UCE), also referred to as "SPAM".

Kephart examines electronic mail for determining if the mail bears patterns of SPAM (i.e junk mail), and blocks such mail. If a message is found as undesirable, the system applies a policy with respect to similar messages, but the whole process is triggered by "determining that transmission or receipt of at least one specific electronic message is undesirable", that is, in a reactive manner. The present invention deals with a conceptually different proactive protection, where the content is not SPAM but rather content having special value to the organization, such as confidential data, secret documents, content protected by copyright, etc. Thus the content being monitored according to exemplary embodiments of the present invention is content stored on databases associated with the local or organizational network. By contrast in Kephart the spam itself is never stored. A signature is made of an initial spam and then the initial spam is discarded, in contrast with the present claim which requires that the content, of which the signature is constructed, is content that was generated on the local or organizational network. The signature is merely

used to prevent further instances of the same spam. Kephart has no interest in the content itself.

Kephart does mention at one location using signatures to detect confidential information, however he provides no disclosure as to how he does this. There is no disclosure in Kephart as to whether this confidential information is stored on a database in the network or whether for example a user sends an email, decides it is confidential and then requests a signature be created to ensure that similar information is not sent out again. That is to say the passing reference in Kephard to confidential information does not indicate whether the confidential information is stored in the local or organizational network or not and the most reasonable scenario that the skilled person would determine from Kephard is that it is not stored on the network because the spam, which is the main embodiment is not. The skilled person would expect that the passing reference is analogous to the main embodiment and that a signature is simply built up from a passing email.

Kephart and the Claims

As explained in the general section above, Kephart does not teach data stored at a local or organizational network whose signatures are also stored therein. That is to say even though Kephart teaches protection of confidential information he merely teaches use of signatures and does not relate to prestored information. Presumably he just checks passing emails, generally newly written, to ensure that they don't cover forbidden subjects.

Kephart does not teach or hint at confidence levels for his comparisons. His comparisons appear to be binary (yes/no) answers directly made on the basis of the signatures, with the sole aim of identifying and filtering spam.

Thus it is maintained that claim 1 as presently amended is novel over Kephart.

In view of the fact that the confidence level includes that referred to in claim 27, the rejection to claims 27 - 30 is now related to. Neither Kephart nor Thomlinson taken separately or together, teaches or even hints at the novel and inventive idea of an apparatus at a local or organizational network where known content stored thereon is to be protected and where a comparison is made between templates or signatures and the content being transported and where the comparison is supported by a confidence level. , as taught by the present application, and defined by the independent claims.

The arguments made above with respect to the novelty and non-obviousness of claim 1 apply *mutatis mutandis* to independent and similarly amended claims 69,109, 110, 125, and 126.

Dependent claims are believed allowable as being dependent on allowable main claim.

Two new independent claims are added. Claim 127 relates to monitoring at the end point. That is to say an individual end point reports that it has been asked to print, send, save etc. The end point reports this state of affairs and the system makes a decision. This is not taught or hinted at in Kephart since the whole idea of Kephart is that the spam should not reach the end point.

Claim 128 includes the making of policy decisions following identification of the confidential information. Kephart does not teach or hint at different policy decisions as per those listed since spam is merely disposed of or isolated.

All of the matters raised by the Examiner have been dealt with and are believed to have been overcome.

In view of the foregoing, it is respectfully submitted that all the claims now pending in the application are allowable. An early Notice of Allowance is therefore respectfully requested.

Respectfully submitted,

Martin D. Moynihan
Registration No. 40,338

Date: October 31, 2007

Enclosures:

- Petition for Extension (Two Months)
- Request for Continued Examination (RCE)